UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte MASAYUKI HATANAKA, JUN KAMADA, TAKAHISA HATAKEYAMA, TAKAYUKI HASABE, SEIGOU KOTANI, TADAAKI TONEGAWA, TAKEAKI ANAZAWA, TOSHIAKI HIOKI, MIWA KANAMORI, and YOSHIHIRO HORI

Appeal 2007-2340
Application 10/069,113
Technology Center 2100

Decided: November 5, 2007

Before JAMES D. THOMAS, KENNETH W. HAIRSTON, and ROBERT E. NAPPI, *Administrative Patent Judges.*

NAPPI, *Administrative Patent Judge.*

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 6(b) (2002) of the final rejection of claims 1 through 18.

We reverse the Examiner's rejections of these claims.

INVENTION

The invention is directed to a recording device which functions as a medium for recording data and functions to prevent unauthorized reproduction, transfer or erasing of the data stored thereon. See page 2 of Appellants' Specification. Claim 1 is representative of the invention and reproduced below:

> 1. A recording device detachably attachable to a reproduction apparatus reproducing and outputting encrypted content data, for receiving and recording said encrypted content data therein, comprising:
>
> a data input/output unit allowing external data communication;
>
> a first storage unit receiving said encrypted content data from said data input/ output unit for storage;
>
> a user information hold unit holding first user ID data provided to identify a user of said recording device;
>
> a protection information memory unit holding protection information updatable in response to a result of comparing externally provided user information with said first user ID data, as externally instructed; and
>
> a control unit controlling an operation of said recording device, said control unit referring to said protection information to restrict external access to said encrypted content data held in said first storage unit.

REFERENCES

Lang	US 5,191,611	Mar. 2, 1993
Hasebe	US 5,392,351	Feb. 21, 1995
Shear	US 2001/0042043 A1	Nov. 15, 2001

REJECTIONS AT ISSUE

Claims 1 through 5 and 13 through 18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Hasebe in view of Lang.

Claims 6 through 12 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Hasebe in view of Lang and Shear.

Throughout the opinion, we make reference to the Brief (received August 18, 2006), Reply Brief (received January 5, 2007) and the Answer (mailed November 7, 2006) for the respective details thereof.

ISSUES

Appellants contend that the Examiner's rejection of claims 1 through 5 and 13 through 18 under 35 U.S.C. § 103(a) is in error. Appellants present several arguments directed to the combination of Hasebe and Lang on pages 7 through 15 of the Brief. Most notably, Appellants argue that the combination of Hasebe and Lang do not teach that the protection information is updatable in response to the result of comparing externally provided user information with the user identification in the user identification hold unit, as recited in claim 1. (Br. 12 and 13).

The Examiner responds in the Answer, stating:

> Appelant [sic, Appellant] has further argued that Lang does not disclose that protection information is updatable in response to a result of comparing externally provided user information with the first user ID data, as edxternally [sic, externally] provided because in the [L]ang the information provider gives the user an updated access code whereas in the claimed invention the user controls the protection of information on the recording device. This feature, again, is not recited in the rejected claims.

(Answer, 11, 12).

In the statement of the rejection, on pages 3 and 4 of the Final Rejection dated January 25, 2006, the Examiner states:

> Hasebe does not disclose the protection information updatable in response to a result of comparing externally provided user information with said first user ID data.
>
> However, Lang teaches a method to distribute content to different recipients (Lang: Abstract) where he teaches comparing stored users information with the user information supplied by a personal access device (PAD) to authorize the updating of user information upon successful authorization (Lang: Col 12 lines 36-58).

Thus, the contentions of the Appellants present us with two issues. First whether claim 1 recites that the protection information is updatable in response to the result of comparing externally provided user information with the user identification in the user identification hold unit. Second, whether the combination of the art applied by the Examiner teaches or suggests this feature.

FINDINGS OF FACT

1. Hasebe teaches a system to protect electronic data, stored on a medium, from illegal copying. (Abstract).
2. Hasebe teaches that the Electronic data is stored on the medium in an encrypted form. The medium also stores the electronic data key which only decrypts the data permitted by the vendor (permission information.) This data key is also encrypted. (Col. 1, l. 62 – col. 2, l. 5, see also figures 1 and 2).
3. Hasebe teaches that the prior art systems operate such that a personal key is generated by the user's computer based upon the user's personal number. This personal number is also transmitted to the data vendor's computer to generate a personal key. The Vendor's computer then uses this key to encrypt the software

decrypting key which is then sent to the user's computer. The decryption key received by the user's computer is then used in conjunction with the permission information to decrypt the electronic data on the medium. (Col. 3, ll. 35-55).

4. Hasebe teaches an improvement to the prior art. Instead of using a personal number, associated with the user or user's computer, to generate the personal key, a medium number, stored on the medium is used. (Col. 4, ll. 9-20).
5. We find no teaching in Hasebe of comparing the user or medium number to externally input information to make any adjustments to the permitted decryption of the data.
6. Lang teaches a system for granting privileges for securely retrieving data from databases. (Abstract).
7. Lang's system may also be applied to information on storage medium. (Col. 2, ll. 25-42).
8. Lang's system makes use of a storage accessing device, a smart card which contains a personal ID code and a personal key. (Col. 2, ll. 42-48).
9. The storage medium contains the data in different zones. Different levels of user access are determined by the zone of the data. Zone Access Codes (ZAC) are assigned to each zone of data. The storage medium stores the ZAC along with identification codes assigned a Personal Unique Key (PSK). (Lang, col. 2, l. 59- col. 3, l. 10).
10. When a user accesses data, using Lang's system, they first enter their personal ID code into the smart card. The smart card then

displays the ZAC and system identification code, which the user enters into a storage computer. The computer system compares the input codes to the codes on the storage medium. If there is a match, the computer retrieves the personal security key and generates a random number which is displayed on the screen. The user inputs the random number into the smart card which uses the input random number and an encryption algorithm to generate a value displayed on the smart card display. The user then inputs the value displayed on the smart card into the computer. The computer compares the input value with a value calculated using the random number and similar encryption algorithm. If there is a match the user is granted access to the data. (Lang col. 3, ll. 20-51).

11. Lang also teaches that this system can be used for remote metering by programming the smart card to provide a limited number of retrievals of the data. In such an application, the user can contact the data provider to obtain an update code which modifies the permissions to allow a user to obtain further access to the data. (Col. 12, ll. 36-59).

12. We find no discussion in Lang about the permissions (protection data) to allow the user to access the data being changed based upon a comparison of external input with an ID value stored on the medium.

ANALYSIS

The first issue we consider is whether claim 1 recites that that the protection information is updatable in response to a result of comparing

externally provided user information with the user identification in the user identification hold unit. Claim 1 recites, "a protection information memory unit holding protection information updatable in response to a result of comparing externally provided user information with said first user ID data, as externally instructed." Claim 1 further recites that the control unit refers to the protection information to restrict access to the encrypted data. Thus, the "protection information" is functionally related to the device as it is referred to in restricting access to data. Claim 1 additionally identifies that, based upon a comparison of externally provided user information with the user ID stored in the user information holding unit, the protection information is updatable. Thus, contrary to the statements by the Examiner on pages 11 and 12 of the Answer, we consider the scope of independent claim 1 to include that protection information is updatable in response to a result of comparing externally provided user information with the user identification in the user identification hold unit.

The second issue we consider is whether the combination of the art applied by the Examiner teaches or suggests this limitation. As discussed above we find that both Lang and Hasebe teach systems for restricting access to electronic data stored on a medium. (Facts 1 and 7). Lang teaches comparing externally input values with values presorted on the medium. (Fact 10). While Lang does teach that the information used to access the medium can be changed (i.e. renew privileges), we do not find that Lang teaches that such changes are updated based upon the comparison of external values with stored values. (Facts 11 and 12). Thus, we do not find that the combination of Lang and Hasebe teaches the limitations of independent claim 1 and we reverse the Examiner's rejection.

Claims 2 through 5 and 13 through 18 are ultimately dependent on claim 1 and similarly are rejected under 35 U.S.C. § 103(a) as being unpatentable over Hasebe in view of Lang. Thus, we reverse the Examiner's rejection of these claims for the same reasons as discussed with respect to claim 1.

The Examiner's rejection of dependent claims 6 through 12 relies upon Lang to teach modifying Hasebe's system. We do not find that the Examiner's additional reliance upon Shear remedies the deficiencies noted in the rejection of claim 1. Accordingly, we will not sustain the Examiner's rejection of claims 6 through 12 under 35 U.S.C. § 103(a).

CONCLUSION

We consider the Examiner's rejections of claims 1 through 18 through under 35 U.S.C. § 103(a) to be in error as we do not find that the combination of applied references teaches or suggests the limitations in independent claim 1and it's dependents.

ORDER

For the foregoing reasons, we will not sustain the Examiner's rejections under 35 U.S.C. § 103. The decision of the Examiner is reversed.

REVERSED

eld

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 CONNECTICUT AVENUE, NW
SUITE 700
WASHINGTON DC 20036